THE UNIFORM PRIMALITY CONJECTURE FOR ELLIPTIC CURVES

GRAHAM EVEREST, PATRICK INGRAM, VALÉRY MAHÉ, SHAUN STEVENS.

Abstract. An elliptic divisibility sequence, generated by a point in the image of a rational isogeny, is shown to possess a uniformly bounded number of prime terms. This result applies over the rational numbers, assuming Lang's conjecture, and over the rational function field, unconditionally. In the latter case, a uniform bound is obtained on the index of a prime term. Sharpened versions of these techniques are shown to lead to explicit results where all the irreducible terms can be computed.

1. Introduction

The Mersenne problem asks if infinitely many integers of the form $2^n - 1$ are prime. More generally, if $a > b$ are positive coprime integers, one can ask if the sequence

$$V_n = \left(\frac{a^n - b^n}{a - b}\right)_{n \geqslant 1} \tag{1}$$

has infinitely many prime terms. The answer is negative if a/b is a perfect power. For example, if $a = A^2$ and $b = B^2$, with A and $B \in \mathbb{Z}$, then the terms factorize as

$$V_n = \left(\frac{A^n - B^n}{A - B}\right)\left(\frac{A^n + B^n}{A + B}\right)$$

for n odd and

$$V_n = \left(\frac{A^n - B^n}{A^2 - B^2}\right)(A^n + B^n)$$

for n even. It is easy to see that neither factor may be a unit when n is large enough. Indeed, since the greatest common divisor of the two terms on the right (in either expression) is easily controlled, there are few possibilities for V_n to be a prime power, a remark germane to this paper.

Let $E/\mathbb{Q}$ denote an elliptic curve, given by a Weierstrass equation with integer coefficients, and let $P \in E(\mathbb{Q})$ denote a non-torsion point. One can

1991 *Mathematics Subject Classification.* 11G05, 11A41.

Key words and phrases. Canonical height, divisibility sequence, division polynomial, elliptic curve, isogeny, prime, rational function field, reduction, Siegel's Theorem.

The research of the second author was supported by grant from NSERC of Canada and one from the LMS. The research of the third author was supported by a grant from EPSRC.

always write

$$nP = \left(\frac{A_n}{B_n^2}, \frac{C_n}{B_n^3}\right),$$

with A_n, B_n, and $C_n \in \mathbb{Z}$, and $\gcd(A_n, B_n) = 1$. The sequence $(B_n)_{n\geqslant 1}$ is an *elliptic divisibility sequence*. These sequences have been the focus of attention of a number of authors: consult [3, 5, 6, 7, 8, 13, 23, 24, 29, 30, 31, 32, 33]. The role of an elliptic divisibility sequence relative to the addition law of $E(\mathbb{Q})$ is analogous to the role of the sequence (1) relative to the multiplicative group of $\mathbb{Q}$. It is unlikely that B_n will ever be prime, because of the relation $B_1 \mid B_n$. It is natural, as in the multiplicative case, to ask when B_n/B_1 might be prime, or a prime power.

1.1. **Background.** Chudnovsky and Chudnovsky [2] considered the question of prime occurrence in elliptic divisibility sequences computationally, finding some examples of prime values which are large (several hundred decimal digits) in comparison with the starting data. These computations were not easy on several counts. For one thing, the terms grow very rapidly - the logarithm is quadratic in the index, and proportional to the global canonical height. Also, there was a shortage of known small height points. Finally, the computing power at the time was much less than what is available today. With the examples to hand, searching was feasible only out to index around $n = 100$. Much larger prime terms in elliptic divisibility sequences have been found recently.

Example 1.1. Consider

$$E : y^2 + y = x^3 - x \text{ with } P = [0, 0].$$

The following table shows indices n for which B_n is prime (actually, a Miller-Rabin pseudo-prime to 10 randomly chosen bases), together with the number $\#B_n$ of decimal digits of B_n:

n	5	7	8	9	11	12	13	19	23	29	83	101	409	1291
$\#B_n$	1	1	1	1	2	2	2	4	6	10	77	114	1857	18498

The final two primes were found by Bríd Ní Fhlathuín (1999) and the first author (2006) respectively using MAGMA [17] and PARI-GP [21]. The largest takes a couple of hours to test for (pseudo-) primality.

Bearing in mind that all of these examples have appeared at the outer limits of what is computationally feasible, at the time, this might suggest that some elliptic divisibility sequences contain infinitely many prime terms. On the other hand, in [5], all of the examples from [2] were tested out to $n = 500$ but no more prime terms appeared. Furthermore, while it is true that the primes in Example 1.1 are large, this sequence has, up to the present, produced only 14 prime terms. It also manifests a pattern witnessed in several examples (see the table in section 4.2), namely, that a *gap principle* seems to be at work. What this means is that the gaps between prime terms grow quickly in proportion to the index. Taking this

together with the quadratic exponential growth rate of the sequence forces any outlying prime term to be inordinately large. In section 4.2, the results of extensive computations are exhibited, showing the appearance of prime terms in elliptic divisibility sequences generated by the 18 rational points with smallest known global canonical height in Elkies' table [10]. These, together with all the computations performed for this paper, used both [17] and [21]. Together with a heuristic argument from [5] (revisited in section 4.1), this indicates that the case of elliptic divisibility sequences could be quite different from that of the multiplicative sequences (1), and lends support to what we believe could be true, namely:

Conjecture 1.2. If $B = (B_n)$ denotes an elliptic divisibility sequence generated by a rational point on an elliptic curve in minimal form, then the number of prime terms B_n/B_1 is uniformly bounded, independent of curve and point.

In [7] it was demonstrated that if $P \in E(\mathbb{Q})$ lies in the image of a non-trivial isogeny then B_n can be prime (indeed a prime power) for only finitely many n. When the isogeny is the endomorphism $[k]$ (multiplication by the integer k), this is in direct analogy with the trivial case for sequences of the form (1), discussed earlier. The proof follows by giving a preliminary argument showing the existence of a canonical factorization, then estimates arising from a strong form of Siegel's Theorem show that each factor is too large to be a unit.

In the current article, a proof of Conjecture 1.2 will be provided, assuming Lang's Conjecture, in the case where P lies in the image of a non-trivial isogeny. The methods include the use of a quantitative version of Siegel's Theorem proved by Silverman. As the question entails the application of results from diophantine approximation, it is also interesting to consider the problem over the function field $\mathbb{Q}(T)$, where stronger diophantine approximation results are known (for example, Lang's Conjecture). Stronger conclusions do indeed become possible.

1.2. **Main Results.** Let K be $\mathbb{Q}$ or $\mathbb{Q}(t)$, and let $\mathcal{O}_K$ be $\mathbb{Z}$ or $\mathbb{Q}[t]$ respectively. Let E be an elliptic curve over K and $P \in E(K)$; then we can write

$$x(P) = \frac{A_P}{B_P^2},$$

with $A_P, B_P \in \mathcal{O}_K$ coprime and $B_P > 0$ in the case $K = \mathbb{Q}$, or B_P monic in the case $K = \mathbb{Q}(t)$.

Much of the discourse assumes a conjecture of Lang, which arises naturally, and appears to be a necessary assumption in any attempt to solve Conjecture 1.2. This conjecture will now be stated and relies upon definitions provided in full in section 2.1. It is known that the canonical height $\hat{h}(P)$ is zero if and only if P is a point of finite order, so it is natural to ask how small $\hat{h}(P)$ might be for non-torsion points P. This question turns

out to be quite important: in general, quantitative estimates for diophantine approximation on elliptic curves all rely on some sort of lower bound on $\hat{h}(P)/h(E)$, where $h(E)$ is the height of the curve. Considering elliptic curves in general, it is not hard to show that $\hat{h}(P)/h(E)$ can be made arbitrarily small (without resorting to choosing torsion points P). For minimal curves E/K, however, this seems not to be the case.

Lang's Conjecture. *There exists $\delta > 0$, which depends only on K, such that $\hat{h}(P) \geqslant \delta \max\{1, h(E)\}$, for all minimal curves E/K and all non-torsion points $P \in E(K)$.*

Our main results use a definition which appeared first in [7] and in a more general form in [6]. In [7], some crude counting amongst small conductor curves suggested that when $K = \mathbb{Q}$, the definition applies in a very large number of non-trivial cases.

Definition 1.3. If $P \in E(K)$ is non-torsion and is the image of a K-rational point under a non-trivial K-rational isogeny, then say that P is *magnified*.

By composing the pre-image of the isogeny with an isomorphism if necessary, it may always be arranged that the pre-image is in minimal form. This will be a standing assumption throughout the paper.

In the rational case, the main theorem of the paper follows (see Theorem 2.1 for a more precise version):

Theorem 1.4. *Assume $K = \mathbb{Q}$ and B is an elliptic divisibility sequence generated by a magnified K-rational point on an elliptic curve in minimal form. If Lang's conjecture holds then the number of prime power terms B_n/B_1 is bounded independently of the curve, the point and the degree of the isogeny.*

When $K = \mathbb{Q}(t)$, as anticipated, an unconditional version of Theorem 1.4 holds. A bigger surprise is the different character of the main conclusion.

Theorem 1.5. *Assume $K = \mathbb{Q}(t)$ and B is an elliptic divisibility sequence arising from a magnified K-rational point on an elliptic curve in minimal form. Then B_n/B_1 fails to be a prime power for all indices $n \geqslant 4160366$.*

The different nature of the two results is worthy of comment and sections 3 and 4 are given over to a full discussion of the different cases. At this point, the following question seems worth asking, it is one that we have not been able to resolve.

Question In the case when $K = \mathbb{Q}$, assume that B is an elliptic divisibility sequence generated by a magnified K-rational point on an elliptic curve in minimal form. If Lang's conjecture is true, does it follow that B_n/B_1 fails to be a prime power for all n beyond some uniform bound?

A positive answer to this question is certainly desirable, because it means that a large class of explicit examples can, at least hypothetically, be tested to find all the prime terms. With current techniques, explicit examples do

exist [9] (see also Example 4.1), but for a limited class of curves. Theoretically too, a positive answer is satisfying because it means that the two cases when $K = \mathbb{Q}$ and $K = \mathbb{Q}(t)$ are exactly parallel, assuming the generating point P is magnified. Note however that, over $K = \mathbb{Q}(t)$, the primality conjecture itself is not likely to be true - a discussion, which includes some striking examples, follows in section 3.

In the next section, a proof will be given that, under Lang's conjecture, a uniform bound exists for the number of prime terms B_n/B_1 which applies in both the rational and the function field cases, assuming the elliptic divisibility sequence is generated by a magnified point on a minimal curve. This section highlights the convergence of the two theories. In sections 3 and 4, which follow on, various points of divergence will be discussed, often with reference to explicit examples.

2. The Uniform Primality Conjecture in Both Cases

2.1. **Notation.** The following notation will be standard throughout:

K	either $\mathbb{Q}$ or $\mathbb{Q}(t)$;
$\mathcal{O}_K$	either $\mathbb{Z}$ if $K = \mathbb{Q}$ or $\mathbb{Q}[t]$ if $K = \mathbb{Q}(t)$;
v	a prime of K with completion K_v, ring of integers $\mathcal{O}_v$;
$\log \lvert . \rvert_\infty$	either $\log(\lvert . \rvert)$ if $K = \mathbb{Q}$ or deg if $K = \mathbb{Q}(t)$;
$h(\frac{p}{q})$	the height of $\frac{p}{q}$ defined, for $p, q \in \mathcal{O}_K$ coprime, by $h(\frac{p}{q}) := \max(\log \lvert p \rvert_\infty, \log \lvert q \rvert_\infty)$;
E	an elliptic curve over K
Δ or Δ_E	the discriminant of E;
j or j_E	the j-invariant of E;
$h(E)$	the height $h(E) := \frac{1}{12}\max(h(j), h(\Delta))$ of E;
P	a point of $E(K)$;
$h(P)$	the height $h(P) := \frac{1}{2}h(x(P))$ of P
$\widehat{h}(P)$	the canonical height $\widehat{h}(P) := \lim_{n \longrightarrow \infty} \frac{h(nP)}{n^2}$ of P;

Generally speaking, when the existence of a uniform constant is postulated, what is meant is a constant independent of the choice of the elliptic curve (and the point studied if there is one). Of course, such a constant may depend on the choice of the base field K.

2.2. **Reduction to Siegel's Theorem.** For ease of exposition, define the *Lang ratio* of $P \in E(K)$ to be $\rho(P, E) = \hat{h}(P)/\max\{1, h(E)\}$. Then Lang's conjecture says that there exists $\delta > 0$ such that

$$\rho(P, E) \geqslant \delta,$$

for all minimal curves E/K and all non-torsion points $P \in E(K)$. Silverman [27] has shown, for number fields K, that $\rho(P, E)$ may be bounded

below in terms of the number of primes at which E/K has split multiplicative reduction. Expanding on these ideas, Hindry and Silverman [11] showed that $\rho(P,E)$ may be bounded below in terms of an upper bound on the Szpiro ratio of E/K, that is, the ratio of the log-discriminant of E to the log-conductor. Hindry and Silverman also showed that if K is a one-dimensional function field, then the Szpiro ratio of an S-minimal elliptic curve (where S is a set of primes of K) is bounded above absolutely in terms of S; in particular, with $S=\{\infty\}$, Lang's Conjecture holds. In this paper, it will often be convenient to work in terms of $\rho(P,E)$ in order to obtain unconditional results.

The following is a more precise version of Theorem 1.4, valid both for $\mathbb{Q}$ and for $\mathbb{Q}(t)$.

Theorem 2.1. *For any $\delta>0$, there is a constant M_δ with the following property: Let $B=(B_n)$ be an elliptic divisibility sequence arising from a magnified K-rational point P on an elliptic curve E in minimal form. Write $\sigma: E'\to E$ with E' in minimal form, and $\sigma(P')=P$. If $\rho(P',E')\geqslant\delta$, then the number of prime power terms B_n/B_1 is bounded by M_δ.*

In light of the above-mentioned results of Hindry and Silverman, in the case $K=\mathbb{Q}(t)$, there is a uniform constant $\delta>0$ such that the condition $\rho(E',P')\geqslant\delta$ is always satisfied. If Szpiro's Conjecture holds, then this is true of $K=\mathbb{Q}$ as well.

Similar methods allow a result of the following kind:

Theorem 2.2. *For any $\delta>0$, there is a constant C_δ with the following property: Let $\phi: E'\to E$ be an isogeny of minimal elliptic curves, then for any subgroup $\Gamma'\subseteq E'(\mathbb{Q})$ such that $\min_{P'\in\Gamma'}\{\rho(E',P')\}\geqslant\delta$,*

$$\#\{P\in\phi(\Gamma') : B_P \textit{ is a prime power}\}\leqslant C_\delta^{1+\operatorname{rank}(\Gamma')}.$$

It follows immediately that the number of prime power terms in the sequence $(B_n)_{n\geqslant 1}$ is bounded uniformly. This observation is not nearly as strong as Theorem 2.1 unless one restricts attention to sequences in which $B_1=1$, which are in some sense rare (corresponding to integral points on elliptic curves).

2.3. **Behaviour Under Isogeny.** The first lemma shows how primes behave under isogeny, and demonstrates that the denominators of points in the image of an isogeny admit a canonical factorization - see (6).

Lemma 2.3. *Let E be a minimal elliptic curve defined over K, and let $\sigma: E'\to E$ be an isogeny of degree m. Then we have*

$$v\left(B_P\right)\leqslant v\left(B_{\sigma(P)}\right).$$

If E' is also minimal, then $v(B_P)>0$ implies

$$v\left(B_{\sigma(P)}\right)\leqslant v\left(B_P\right)+v(m).$$

Proof. On the assumption that E' is minimal at v, it is not hard to show (see, for example, the exposition in [32]) that the isogeny σ induces a map of formal groups $F_\sigma : \hat{E}' \to \hat{E}$ defined over $\mathcal{O}_v$ with $F_\sigma(0) = 0$ (Streng proves this for number fields, but the proof works for any local field). It follows immediately that if $v(x(P)) < 0$, as $F_\sigma(z) \in \mathcal{O}_v[[z]]$ vanishes at 0,

$$v(B_{\sigma(P)}) = v(F_\sigma(z)) \geqslant v(z) = v(B_P).$$

If E is minimal as well, we may apply the same argument to the dual isogeny $\hat{\sigma} : E \to E'$, noting that the composition is $[m]$. The argument above now tell us that

$$v(B_{\sigma(P)}) \leqslant v(B_{mP}) \leqslant v(B_P) + v(m).$$

□

Lemma 2.4. *Let E and E' be minimal elliptic curves defined over K, and let $\sigma : E' \to E$ be an isogeny of degree m. Then*

$$h(E) \ll h(E') + h(m).$$

Proof. In the number field case, this is a consequence of the Normalizing Lemma of Masser and Wüstholz [19]. Note that Masser and Wüstholz use the quantity

$$w(E) = \max\{1, h(g_2), h(g_3)\}$$

to measure the 'size' of an elliptic curve, where g_2 and g_3 are the usual invariants, but $h(E)$ as defined above satisfies $w(E) \ll h(E) \ll w(E)$. The argument in [19] produces *some* isomorphic copy of E, say E^*/K such that $h(E^*) \ll h(E') + \log m$. Since E and E^* are isomorphic, and E is minimal, we have $h(E) \leqslant h(E^*)$.

If K is a function field, this property is trivial by the boundedness of the Szpiro ratio, together with the inequality $\deg(\Delta_{E'}) \leqslant 6\deg(\Delta_E)$. To see this, note first that E and E' have the same conductor, by [12, VII Corollary 7.2]. The assertion is then a consequence of [22, Theorem 0.1], which bounds the conductor of E' in terms of $6\deg(\Delta_{E'})$, since the degree of the conductor of E is a lower bound for $\deg(\Delta_E)$. Note that if we assume the *abc* conjecture for K, we may do the same thing for number fields, but a dependence on m still exists. □

Now we return to the main theme of this section, by showing how to reduce the problem to an application of Siegel's Theorem.

Definition 2.5. Given $0 < \varepsilon < 1$, together with a constant $C > 0$, say that $P \in E(K)$ is (ε, C)-*quasi-integral* if

$$h(B_P) \leqslant \varepsilon\hat{h}(P) + C.$$

Siegel's Theorem, in its strong form, is the statement that for any $\varepsilon < 1$ and any constant C, there are only finitely many (ε, C)-quasi-integral points in $E(K)$. Work of Silverman [27] refines this claim, showing that the number of (ε, C)-quasi-integral points in a subgroup $\Gamma \subseteq E(K)$ may be bounded

solely in terms of ε, C, $\operatorname{rank}(\Gamma)$, and a lower bound on $\rho(P,E)$ for non-torsion $P \in \Gamma$. Elliptic divisibility sequences are essentially rank one subgroups of $E(K)$, and so under Lang's Conjecture a uniform bound is obtained on the number of (ε, C)-quasi-integral points in an elliptic divisibility sequence. Note that if

$$Ch(E) > \delta \hat{h}(nP),$$

then $|n| \leqslant \sqrt{C/(\delta\rho(P,E))}$.

In particular, applying Silverman's version of Siegel's Theorem to a rank-one subgroup of $E(K)$ generated by some point P with $\rho(P,E)$ greater than some uniform value, some dependence of C on E is acceptable (in the sense that a uniform quantitative result is recoverable), as long as $C = O(h(E))$.

It will be demonstrated that if P is the image of a K-rational point under an isogeny, then B_{nP}/B_P being a power of a prime is a non-trivial quasi-integrality condition. The function field case indicates that one would not expect this to be true more generally.

Lemma 2.6. *Let $\sigma : E' \to E$ be an isogeny of minimal elliptic curves over K, and suppose that $P = \sigma(P')$ for some $P' \in E'(K)$. If B_{nP}/B_P is a power of a single prime, then either nP is (ε_1, C_1)-quasi-integral, with $\varepsilon_1 = \frac{1}{n^2} + \frac{1}{m}$ and $C_1 = O(h(E) + h(m) + h(n))$, or nP' is (ε_2, C_2)-quasi-integral, with $\varepsilon_2 = \frac{m}{n^2}$ and $C_2 = O(h(E') + h(m))$.*

Proof. Suppose that B_{nP}/B_P is a power of a single prime. Note that, by Lemma 2.3, $v(B_{nP'}) \leqslant v(B_{nP})$ for all $v \in M_K^0$. Suppose, for the moment, that $v(B_{nP'}) \leqslant v(B_P)$ for all $v \in M_K^0$. In this case,

$$\begin{aligned} h(B_{nP'}) &\leqslant h(B_P) \\ &\leqslant h(P) \\ &\leqslant \hat{h}(P) + O(h(E)) \\ &\leqslant \frac{m}{n^2}\hat{h}(nP') + O(h(E') + h(m)). \end{aligned}$$

Now suppose that this is not the case, in other words, $v(B_{nP'}) > v(B_P)$ for some prime $v \in M_K^0$. Then $v(B_{nP}/B_P) > 0$, and this is the only prime for which this happens. Furthermore, from Lemma 2.3

$$v(B_{nP}/B_P) \leqslant v(B_{nP}) \leqslant v(B_{nP'}) + h(m).$$

In particular,

$$\begin{aligned} h(B_{nP}) &\leqslant h(B_P) + h(B_{nP'}) + h(m) + h(n) \\ &\leqslant \hat{h}(B_P) + \hat{h}(B_{nP'}) + O(h(E) + h(E') + h(m) + h(n)) \\ &\leqslant \left(\frac{1}{n^2} + \frac{1}{m}\right)\hat{h}(nP) + O(h(E) + h(m) + h(n)). \end{aligned}$$

□

It has been known for a long time that sequences of the form (1) do produce new primes in a weaker sense. Zsigmondy's Theorem [34] guarantees

a new prime factor for all terms with index $n > 6$. The definition is made precise now.

Definition 2.7. A nonzero term B_n in a sequence (B_n) of elements in $\mathcal{O}_K$ has a *primitive divisor* d if

(I) d is not a unit
(II) $d \mid B_n$
(III) $\gcd(B_m, d)$ is a unit for all $m < n$ with $B_m \neq 0$.

Silverman [28] proved the elliptic analogue of Zsigmondy's Theorem: in any elliptic divisibility sequence $B = (B_n)$, all the terms from some index onwards will have a primitive divisor. This theorem has been proved in a strong uniform manner in [16] (see also [8] and [13]) and and will be used crucially in the following proof.

Proof of Theorem 2.1 in the rational case. It will be shown that for every $\delta > 0$ there is a constant M_δ depending only on δ such that for every pair of minimal elliptic curves $E', E/\mathbb{Q}$ equipped with a non-trivial isogeny $\sigma : E' \to E$, and every point $P = \sigma(P')$ with $\rho(P', E') \geqslant \delta$, there are at most M_δ values n such that B_{nP}/B_P is a prime power.

The style of proof depends upon whether the isogeny is cyclic. Firstly, assume that $P \in kE(\mathbb{Q})$ for some integer $k \geqslant 2$. Then $P \in qE(\mathbb{Q})$ for some prime q, and it may be assumed that k is prime.

Suppose there are distinct non-archimedean valuations v_1 and v_2 such that

$$v_1(B_{nkP'}) > 0 \quad \text{and} \quad v_1(B_{kP'}) = 0$$

and

$$v_2(B_{nP'}) > 0 \quad \text{and} \quad v_2(B_{\gcd(k,n)P'}) = 0.$$

Then clearly $v_1(B_{nP}/B_P) > 0$. On the other hand, $v_2(B_{kP'}) = 0$, as

$$v_2(B_{\gcd(k,n)P'}) = \min\{v_2(B_{nP'}), v_2(B_{kP'})\},$$

and so $v_2(B_{nP}/B_P) > 0$. Thus if B_{nP}/B_P is a prime power, then either:

(a) the primes diving $B_{nkP'}$ are at most those dividing $B_{kP'}$ or
(b) the primes diving $B_{nP'}$ are at most those dividing $B_{\gcd(k,n)P'}$.

Let $Z(P', E')$ denote the set of s such that $B_{sP'}$ has no prime divisors other than those dividing $B_{tP'}$ for $t < s$. In case (a), the term $B_{nkP'}$ in the elliptic divisibility sequence defined by P' has no primitive divisor, and so $nk \in Z(P', E')$. If (b) holds, and if $\gcd(k, n) < n$, then $n \in Z(P', E')$. Thus, if B_{nP}/B_P is a prime power, then either $n \mid k$ (and recall that k is assumed to be prime) or $n \in Z(P', E') \cup \frac{1}{k} Z(P', E')$. By Theorem 7 of [16], $\#Z(P', E')$ may be bounded solely in terms of $\rho(P', E')$ (Note that the statement in [16] is not in terms of $\rho(P', E')$, but a simple modification of the proof shows that this is true). Thus the number of n such that B_{nP}/B_P is a prime power is bounded by some $M_{\delta,1}$ which depends only on δ.

So now suppose $P \notin kE(\mathbb{Q})$ for any integer $k \geqslant 2$. It follows that σ is a composition of cyclic isogenies over $\mathbb{Q}$, and so it may be assumed (without loss of generality) that σ itself is cyclic. In particular, there are (by work of Mazur [20]) only finitely many possible values for $m = \deg(\sigma)$. Thus Lemma 2.6, replacing $h(m)$ with a sufficiently large constant, tells us that if B_{nP}/B_P is a prime power, then either nP is (ε_1, C_1)-quasi-integral, with $\varepsilon_1 = \frac{1}{n^2}+\frac{1}{m}$ and $C_1 = O(h(E)+h(n))$, or nP' is (ε_2, C_2)-quasi-integral, with $\varepsilon_2 = \frac{m}{n^2}$ and $C_2 = O(h(E'))$. If $\frac{m}{n^2} \leqslant \frac{3}{4}$, there is a bound on the number of points satisfying the latter condition depending only on $\rho(P', E')$. Clearly the number of n such that $\frac{m}{n^2} > \frac{3}{4}$ is bounded absolutely.

Now note that $\rho(P', E') \geqslant \delta$ and Lemma 2.4 implies that $\rho(P, E) \geqslant \delta_2$ for some $\delta_2 > 0$. Thus, the first condition above becomes

$$h(B_{nP}) \leqslant \left(\frac{1}{n^2} + \frac{1}{m}\right) \hat{h}(nP) + O(h(E) + h(n)).$$

Finally, for any C and any $\delta_3 > 0$, we can ensure that $Ch(n) < \delta_3 \hat{h}(nP)$ by taking n large enough. Thus the above becomes

$$h(B_{nP}) \leqslant \left(\frac{1}{n^2} + \frac{1}{m} + \delta_3\right) \hat{h}(nP) + O(h(E))$$

for sufficiently large n, where δ_3 may be taken as any positive value. Applying the quantitative Siegel Theorem, the proof is complete. □

Remark 2.8. Work of the second author [14, 15], in the case $K = \mathbb{Q}$, also assuming Lang's Conjecture, can be applied to produce a uniform bound M such that for any elliptic divisibility sequence generated by a magnified point P on a minimal curve, there are at most two values $n > M$ such that B_{nP} is a prime power.

In the function field case, a stronger version of Theorem 2.1 will be proved, namely, that there is a uniform bound N_0 such that B_n/B_1 is not a prime power for all $n \geqslant N_0$. First, one lemma is required.

Lemma 2.9. *Let $K = \mathbb{Q}(t)$ and let $B = (B_n)$ be an elliptic divisibility sequence arising from a non-torsion point on a minimal elliptic curve defined over K. There is a uniform bound on the indices n for which B_n fails to have a primitive divisor.*

Lemma 2.9 will be proved in an explicit way later – see Theorem 3.10.

Proof of Theorem 2.1 in the function field case. Lemma 2.6 shows that if B_{nP}/B_P is a prime power, then

$$h(B_{nP}) \leqslant \left(\frac{1}{m} + \frac{1}{n^2}\right) \hat{h}(nP) + O(h(E))$$

or

$$h(B_{nP'}) \leqslant \left(\frac{m}{n^2}\right) \hat{h}(nP') + O(h(E')).$$

If $n \geqslant \sqrt{2m}$ and $m \geqslant 2$, then this implies
$$h(B_{nP}) \leqslant \frac{3}{4}\hat{h}(nP) + O(h(E))$$
or
$$h(B_{nP'}) \leqslant \frac{1}{2}\hat{h}(nP') + O(h(E')),$$
respectively. As $\rho(E,P)$ and $\rho(E',P')$ may be bounded below by some absolute, positive value, it follows that the number of such n must be bounded uniformly.

To show that n itself must be bounded, note that if $P \in kE(\mathbb{Q}(t))$ for some integer $k \geqslant 2$ then the existence of a primitive divisor may be used exactly as in the proof in the rational case – the boundedness of n follows using Lemma 2.9. In the case of a cyclic isogeny, the structure of the proof follows the rational case. The differences are: Lang's conjecture is known to be true; a uniform bound for the degree of the isogeny follows from the existence of the same in the rational case since, for any isogeny over of elliptic curves over $\mathbb{Q}(t)$, some specialization will be an isogeny of elliptic curves over $\mathbb{Q}$; and Lemma 2.9 implies a quantitative Siegel Theorem in which the index n is bounded. $\square$

That n itself may be bounded in the above argument is already suggested by Proposition 8.2 of [11]. In Section 3 below we will work out some explicit bounds, in particular the explicit bound given in Theorem 1.5.

3. The Function Field Case

3.1. **Explicit Bounds for $\mathbb{Q}(t)$.** Over $\mathbb{Q}(t)$, Theorem 1.5 raises the possibility of finding all the irreducible terms in particular cases. The bound of 4160366 comes from applying the general version of Lang's conjecture [11], assuming also the maximal possible degree for a cyclic isogeny. As it stands, this is useless: checking the terms coming from smaller indices involves testing rational polynomials for irreducibility which have degrees well in excess of one billion. In particular cases, the problem is circumvented by obtaining a more nuanced version of Lang's conjecture (which takes account of the reduction of small multiples of P, see Theorem 3.5) together with Theorem 3.12, which highlights the dependence upon the degree of the isogeny. This technique allows us to exhibit examples of elliptic divisibility sequences where all of the prime (= irreducible) terms can be computed.

Example 3.1. Consider
$$E : y^2 = x^3 + t^2(1-t^2)x \text{ with } P = [t^2, t^2].$$
Then $B_n/B_1 = B_n$ fails to be a prime power for all $n \geqslant 3$. Note that the point P is magnified by a 2-isogeny as detailed in [1, Chapter 14].

On the other hand, it is worth probing the deeper difference between the cases when $K = \mathbb{Q}$ and $K = \mathbb{Q}(t)$ which is probably at work in general. It is easy to prove that the polynomial $(t^n-1)/(t-1)$ is irreducible for every

prime index n. An analogous statement seems to be true for some elliptic divisibility sequences over function fields. The two curves in Example 3.2 appeared in [11] as examples where the global canonical height of a point is small:

Example 3.2. The point $P = [0, 0]$ on the curve

$$E : y^2 + xy + (t + 1)t^2y = x^3 + t^2x^2$$

produces terms B_{nP} which are irreducible for all primes n from 5 to 199. The point $P = [0, 0]$ on the curve

$$E : y^2 + xy + (t + 1)t^3y = x^3 + t^3x^2$$

produces terms B_{nP} which are irreducible for all primes n from 5 to 199.

More surprisingly, there seem to be examples where irreducibility occurs along prime indices in a fixed residue class.

Example 3.3. The point $P = [1 - t, 1 - t]$ on the curve

$$E : y^2 = x^3 + t(1 - t)x$$

produces irreducible terms B_{nP} whenever $n \leqslant 79$ is a prime congruent to 3 (mod 4).

That B_{nP} is composite for any prime $n \equiv 1 \pmod 4$ is not surprising, in light of results of Streng [32] for elliptic divisibility sequences arising from elliptic curves (over number fields) with complex multiplication.

3.2. **Lang's conjecture.**

We do *not* propose to make explicit the argument given in section 5. Instead, the technique is to work with local heights and explicit bounds for the difference between the naïve and canonical heights. When $K = \mathbb{Q}(t)$ the infinite place ∞ corresponds to the valuation $-\deg$. Without loss of generality, assume that E is given by a short Weierstrass form

$$y^2 = x^3 + Ax + B \tag{2}$$

with $A, B \in \mathbb{Q}[t]$, so that $\Delta_E = -16(4A^3 + 27B^2)$. Then the j-invariant j_E of E is given by

$$j_E = \frac{-1728(4A)^3}{\Delta_E} \tag{3}$$

and the height $h(E)$ of the curve E is

$$h(E) = \frac{1}{12}\max(h(j_E), h(\Delta_E)) = \frac{1}{12}\max(3\deg(A), 2\deg(B)).$$

For v any place of K, denote by $\lambda_v(P)$ the Néron local height of P at v, and by $h_v(P)$ the naïve local height

$$h_v(P) = \frac{1}{2}\max\{0, -v(x(P))\}.$$

The first lemma compares the heights of the j-invariant and discriminant of E.

Lemma 3.4. *With j_E as in (3),*

$$h(j_E) \leqslant \frac{3}{2}\deg(\Delta_E).$$

Proof. Let L be the smallest Galois extension of $\mathbb{Q}(t)$ containing the roots δ_1, δ_2 and $\delta_3 = -\delta_1 - \delta_2$ of $x^3 + Ax + B$. Let v be a place of L above the place at infinity. Since $x^3 + Ax + B$ is monic with polynomial coefficients, $v_{\mathcal{P}}(\delta_i) \geqslant 0$, for every finite place $\mathcal{P}$ of L, so that $v_{\mathcal{P}}(\delta_i - \delta_j) \geqslant 0$. Summing over all finite places of L, and using the fact that $\delta_i - \delta_j$ has the same valuation at all places of the Galois extension L above the infinite place, it follows that $v(\delta_i - \delta_j) \leqslant 0$.

Since v is non-archimedean, at most one of the valuations $v(\delta_1 - \delta_2)$, $v(2\delta_1 + \delta_2)$ and $v(\delta_1 + 2\delta_2)$ can be different from $\min(v(\delta_1), v(\delta_2))$. In particular, since $\Delta_E = ((\delta_1 - \delta_2)(2\delta_1 + \delta_2)(\delta_1 + 2\delta_2))^2$, it follows that $v(\Delta_E) \leqslant 4\min(v(\delta_1), v(\delta_2))$. Hence

$$v(B^2) = 2(v(\delta_1) + v(\delta_2) + v(\delta_1 + \delta_2)) \geqslant 6\min(v(\delta_1), v(\delta_2)) \geqslant \frac{3}{2}v(\Delta_E).$$

Summing over all places v of L above the place at infinity gives

$$\deg(B^2) \leqslant \frac{3}{2}\deg(\Delta_E).$$

The lemma is now a consequence of the inequality

$$\deg(A^3) \leqslant \max(\deg(B^2), \deg(\Delta_E)) \leqslant \frac{3}{2}\deg(\Delta_E)$$

together with the definition $j_E = \frac{-1728(4A)^3}{\Delta_E}$ of the j-invariant of E. □

The following is a version of Lang's conjecture, which was proved in the function field case by Hindry–Silverman [11]. The explicit constants obtained here, in certain special cases, use the same basic methods.

Proposition 3.5. *There is a constant $c > 0$ such that, for all non-torsion points $P \in E(K)$,*

$$c\deg(\Delta_E) \leqslant \widehat{h}(P),$$

where c can be taken to be the following:

- *in the general case, $c = 10^{-9.2}$;*
- *if P has everywhere good reduction, $c = \frac{1}{12}$;*
- *if P has everywhere good reduction except at infinity, $c = \frac{1}{16}$;*
- *if E does not have split multiplicative reduction (in particular, if E is isotrivial), $c = \frac{1}{1728}$;*
- *if E does not have split multiplicative reduction except at infinity (in particular, if E has a polynomial j-invariant), $c = \frac{1}{2304}$.*

Proof. The first bound is the second remark on Theorem 6.1 in [11]. Assume now that P has everywhere good reduction except maybe at infinity. Let v be a valuation different from the valuation at infinity. The coefficients of

the chosen Weierstrass equation are polynomials. Following [18, III Theorem 4.5], the Néron local height λ_v at v satisfies

$$\lambda_v(P) = \frac{1}{2}\max\{-v(x(P)), 0\} + \frac{1}{12}v(\Delta_E) \geqslant \frac{1}{12}v(\Delta_E),$$

while the Néron local height λ_∞ at infinity satisfies

$$\lambda_\infty(P) \geqslant \frac{1}{2}\max\{0, \deg(X(P))\} + \frac{1}{24}\min\{0, -h(j_E)\} \geqslant -\frac{1}{24}h(j_E),$$

for some function X on $E(K)$. Summing over all places gives

$$\widehat{h}(P) \geqslant \frac{1}{12}\deg(\Delta_E) - \frac{1}{24}h(j_E).$$

In particular, Lemma 3.4 implies

$$\widehat{h}(P) \geqslant \left(1 - \frac{1}{4}\right)\frac{1}{12}\deg(\Delta_E) = \frac{1}{16}\deg(\Delta_E)$$

and the third bound follows.

Now assume P also has good reduction at infinity. Since the coefficients in the Weierstrass equation are not integral at infinity, a transformation is needed to an ∞-minimal Weierstrass equation, with discriminant Δ_∞. Since the Néron local height does not depend on the choice of Weierstrass equation,

$$\lambda_\infty(P) \geqslant \frac{1}{12}v_\infty(\Delta_\infty) \geqslant 0.$$

Summing over all places as before,

$$\widehat{h}(P) \geqslant \frac{1}{12}\sum_{v\neq\infty} v(\Delta_E) = -\frac{1}{12}v_\infty(\Delta_E) = \frac{1}{12}\deg(\Delta_E)$$

which gives the second bound.

When E does not have split multiplicative reduction at v, the Kodaira-Néron Theorem asserts that $12P$ has good reduction at v. Hence the bounds for $\widehat{h}(P)$ and the functoriality of the canonical height $\widehat{h}(12P) = 144\widehat{h}(P)$ give the final two bounds. □

Remark 3.6. In special cases, one can improve the constants in Theorem 3.5 by a more careful analysis of the reduction types at bad primes. Moreover, even when E has split multiplicative reduction, the Kodaira-Néron Theorem gives a good constant also when there is a small common multiple of all the valuations of the discriminant Δ_E (for example if it is squarefree).

3.3. **Naïve and canonical heights.**

In order to estimate the difference between the naïve and canonical heights of a point, pass to the local heights. The most difficult of these is the height at infinity, which is addressed first.

Lemma 3.7. *For $P \in E(K)$,*

$$-\frac{5}{6}-h(E)+\frac{1}{24}\min(0,v_\infty(j)) \leqslant \lambda_\infty(P)-h_\infty(P) \leqslant h(E)+\frac{5}{6}-\frac{1}{12}\deg(\Delta_E).$$

Proof. The coefficients A and B of the minimal Weierstrass equation (2) are not v_∞-integral. A Weierstrass equation of E with v_∞-integral coefficients is given by

$$Y^2 = X^3 + t^{-4r}AX + t^{-6r}$$

where r is the smallest integer greater than or equal to $h(E)$. The corresponding change of variables is given by $x = t^{2r}X$ and $y = t^{3r}Y$ and the discriminant of this equation is is $\Delta_\infty = t^{-12r}\Delta_E$.

Following [18, III Theorem 4.5], the Néron local height λ_∞ satisfies

$$\frac{1}{24}\min(0,v_\infty(j)) \leqslant \lambda_\infty(P) - \frac{1}{2}\max(0,-v_\infty(X(P)) \leqslant \frac{1}{12}v_\infty(\Delta_\infty)$$

Since $2\lambda_\infty(P) - r \leqslant \frac{1}{2}\max(0,-2r+\deg(x(P))) \leqslant \lambda_\infty(P)$, this can be reformulated in terms of $x(P)$, Δ_E and r as

$$-r + \frac{1}{24}\min(0,v_\infty(j)) \leqslant \lambda_\infty(P) - h_\infty(P) \leqslant r - \frac{1}{12}\deg(\Delta_E).$$

The integer r is the smallest integer greater than or equal to $h(E)$, which is at most $h(E) + \frac{5}{6}$, and the result follow. □

Now the difference between naïve and canonical heights can be bounded.

Proposition 3.8. *For $P \in E(K)$,*

$$-\frac{3}{16}\deg(\Delta_E) - \frac{5}{6} \leqslant \widehat{h}(P) - h(P) \leqslant \frac{1}{8}\deg(\Delta_E) + \frac{5}{6}$$

Proof. Following [18, III Theorem 4.5], the Néron local height λ_v at any finite place v satisfies

$$\frac{1}{24}\min(0,v(j)) \leqslant \lambda_v(P) - h_v(P) \leqslant \frac{1}{12}v(\Delta_E).$$

Together with Lemma 3.7, and summing over all places, this gives

$$-\frac{5}{6} - h(E) - \frac{1}{24}h(j) \leqslant \widehat{h}(P) - h(P) \leqslant h(E) + \frac{5}{6}.$$

To conclude we notice that $h(j) \leqslant 12h(E)$ and use that $h(E) \leqslant \frac{1}{8}\deg(\Delta_E)$ from Lemma 3.4. □

This subsection concludes with an estimate on the degree of the denominator of $x(P)$, in terms of the (naïve) height of P. This, in particular the fact that the constant $\frac{3}{4}$ is large enough, is crucial to the explicit bounds later.

Lemma 3.9. *For $P \in E(K)$,*

$$\frac{3}{4}h(P) - \frac{3}{16}\deg(\Delta_E) \leqslant \deg(B_P).$$

Proof. This uses a standard approach to Siegel's Theorem. Assume that $h(P) = \frac{1}{2}\deg(A_P)$ (or we are done). Denote by K_∞ the completion of K at the infinite valuation, and by L the algebraic closure of K_∞. Let v be the valuation on L which extends the valuation $-\deg$ on K_∞. Inserting the coordinates of P into the equation for E gives

$$C_P^2 = (A_P - \delta_1 B_P^2)(A_P - \delta_2 B_P^2)(A_P - \delta_3 B_P^2).$$

This may be factored in L as

$$C_i^2 = A_P - \delta_i B_P^2,$$

because the factors of Δ_E are squares in L (so they may be absorbed into the $C_i, i = 1, 2, 3$).

As in the proof of Lemma 3.4, $v(\Delta_E) \leqslant \frac{1}{4}v(\delta_i)$, for each i. If $v(A_P) \geqslant v(\delta_i B_P^2)$ then we have $v(A_P) \geqslant 2v(B_P) + \frac{1}{4}v(\Delta_E)$ and nothing further is needed. So consider the case when $v(A_P) < v(\delta_i B_P^2)$ for $i = 1, 2, 3$, or more precisely the case when

$$v(A_P) = 2v(C_i), \quad i = 1, 2, 3.$$

For $i \neq j$,

$$(\delta_j - \delta_i)B_P^2 = C_i^2 - C_j^2 = (C_i + C_j)(C_i - C_j)$$

therefore

$$B_{ij+}^2 = C_i + C_j \text{ and } B_{ij-}^2 = C_i - C_j,$$

Without loss of generality, assume $v(B_{ij+}) \leqslant v(B_{ij-})$.

We assert that (at least) one of the following two inequalities holds:

$$\begin{aligned} v(B_{12+}) &\geqslant \frac{2}{3}v(B_P) + \frac{1}{2}v(\delta_2 - \delta_1) \quad \text{or} \\ v(B_{13+}) &\geqslant \frac{2}{3}v(B_P) + \frac{1}{2}v(\delta_3 - \delta_1). \end{aligned} \tag{4}$$

To prove this assume that

$$\begin{aligned} v(B_{12+}) &< \frac{2}{3}v(B_P) + \frac{1}{2}v(\delta_2 - \delta_1) \quad \text{and} \\ v(B_{13+}) &< \frac{2}{3}v(B_P) + \frac{1}{2}v(\delta_3 - \delta_1). \end{aligned} \tag{5}$$

This forces

$$v(B_{12-}) > \frac{1}{3}v(B_P) \quad \text{and} \quad v(B_{13-}) > \frac{1}{3}v(B_P).$$

Then Siegel's relation $(C_1 - C_2) + (C_2 - C_3) = C_1 - C_3$ forces

$$v(B_{23-}) > \frac{1}{3}v(B_P).$$

Since $\operatorname{lcm}(B_{12+}^2, B_{13+}^2)$ divides $B_P^2(\delta_2 - \delta_1)(\delta_3 - \delta_1)$, the inequalities (5) imply

$$\begin{aligned} v(\gcd(B_{12+}, B_{13+})) &= v(B_{12+}) + v(B_{13+}) - v(\operatorname{lcm}(B_{12+}, B_{13+})) \\ &< \frac{1}{3}v(B_P). \end{aligned}$$

Now Siegel's relation $(C_1+C_2)-(C_1+C_3) = C_2-C_3$ shows that $\gcd(B_{12+}, B_{13+})$ divides B_{23-}. In particular,

$$\frac{1}{3}v(B_P) < v(B_{23-}) \leqslant \gcd(B_{12+}, B_{13+}) < \frac{1}{3}v(B_P),$$

which is absurd.

Hence one of the inequalities (4) holds, say the first. Since

$$v(B_{12-}) \geqslant v(B_{12+}) \text{ and } 2C_1 = B_{12+}^2 + B_{12-}^2,$$

it follows that

$$\frac{1}{2}v(A_P) = v(C_1) \geqslant \frac{4}{3}v(B_P) + v(\delta_2 - \delta_1) \geqslant \frac{4}{3}v(B_P) + \frac{1}{4}v(\Delta_E).$$

To conclude, recall that v extends $-\deg$. □

3.4. **Primitive divisors.**

Theorem 3.10. *Let $P \in E(K)$ be a non-torsion point and let $B = (B_n)$ be the elliptic divisibility sequence arising from P. There is a uniform constant N_0 such that for all $n \geqslant N_0$, B_n has a primitive divisor.*

- *In general, $N_0 = 190000$.*
- *If P has everywhere good reduction, $N_0 = 7$.*
- *If P has everywhere good reduction except at infinity, $N_0 = 11$.*
- *If E is isotrivial, $N_0 = 133$.*
- *If E has a polynomial j-invariant, $N_0 = 151$.*

Proof. Suppose the term B_n does not have a primitive divisor. Given any irreducible factor f, there is a $d < n$ with $f|B_d$. Since f also divides $B_{\gcd(n,d)}$ we may assume d is actually a divisor of n. What is more, the valuation of B_n and B_d must be the same. It follows that if B_n does not have a primitive divisor then B_n divides $\prod_{p|n} B_{\frac{n}{p}}$; in particular,

$$\deg(B_n) \leqslant \sum_{p|n} \deg(B_{\frac{n}{p}}).$$

Now apply Lemma 3.9 to obtain

$$\frac{3}{4}h(nP) - \frac{3}{16}\deg(\Delta_E) \leqslant \sum_{p|n} h\left(\frac{n}{p}P\right).$$

Proposition 3.8, with the functoriality of the canonical height, gives

$$\frac{3}{4}\left(hn^2 - \frac{1}{8}\deg(\Delta_E) - \frac{5}{6}\right) - \frac{3}{16}\deg(\Delta_E)$$
$$\leqslant hn^2\left(\sum_{p|n}\frac{1}{p^2}\right) + \frac{3}{16}\omega(n)\deg(\Delta_E) + \frac{5}{6}\omega(n),$$

where $\omega(n)$ denotes the number of prime factors of n. Re-arranging, dividing by $\deg(\Delta_E) \geqslant 1$, and applying Lang's conjecture (Proposition 3.5, with c equal to the constant from there) gives

$$cn^2\left(\frac{3}{4} - \sum_{p|n}\frac{1}{p^2}\right) \leqslant \frac{87+98\omega(n)}{96}.$$

Using $\frac{3}{4} - \sum_{p|n}\frac{1}{p^2} \geqslant 0.297$ and $\omega(n) \leqslant \log(n)/\log(2)$, firstly bounds n roughly. Then a more careful analysis of small values of n yields the bounds in the Theorem. □

3.5. **Prime powers.**

Suppose now that E' is another elliptic curve over K, defined relative to a minimal short Weierstrass equation with discriminant $\Delta_{E'}$, and that $\sigma : E' \to E$ is an isogeny of degree $m > 1$. The following is a direct consequence of Lemma 2.3.

Lemma 3.11. *Suppose $P' \in E'(K)$ and $P = \sigma(P')$. Then*

$$B_P = B_{P'}\widetilde{B}_P, \tag{6}$$

with $\widetilde{B}_P$ coprime to $B_{P'}$.

We already know how to deal with isogenies of the form $[k]$ for some integer k, using Theorem 3.10. From now on, we work only with cyclic isogenies. Note that the degree of such an isogeny is bounded as in the rational case (by specialization), $m \leqslant 163$, by Mazur's famous result [20] (see also [25, page 265]). The explicit dependence upon the degree is shown in what follows.

Theorem 3.12. *Suppose $B = (B_{nP})$ is an elliptic divisibility sequence generated by a rational point P on a minimal elliptic curve. Assume P is magnified by a cyclic isogeny of degree m. There are uniform constants N_0 and N_1 such that for all*

$$n \geqslant \max\{N_0, N_1\sqrt{m}\},$$

B_n/B_1 has at least two distinct prime factors.

- *In general, $N_0 = 133034, N_1 = 325865$.*
- *If P' has everywhere good reduction, $N_0 = 12, N_1 = 5$.*
- *If P' has everywhere good reduction except at infinity, $N_0 = 14, N_1 = 6$.*
- *If E' is isotrivial, $N_0 = 140, N_1 = 58$.*
- *If E' has a polynomial j-invariant, $N_0 = 161, N_1 = 67$.*

Proof of Theorem 1.5. The proof follows from Theorem 3.12 for the cyclic case and Theorem 3.10 if the isogeny is $[k]$ for some integer k. The worst possible bound comes from assuming we have a cyclic isogeny of degree 163, together with no other special assumptions. □

Proof of Theorem 3.12. Write $B' = (B'_n)$ for the elliptic divisibility sequence arising from P'. By Lemma 3.11,

$$\frac{B_n}{B_1}.B_1 = B'_n\widetilde{B_n}.$$

If $\deg(B_n/B_1) > \deg(B'_n) > \deg(B_1)$ then B_n/B_1 has two distinct prime factors. Begin with the first inequality. To bound $\deg(B_n/B_1)$ below use Lemma 3.9 and Proposition 3.8. This yields

$$\deg(B_n) - \deg(B_1) > h\left(\frac{3n^2}{4} - 1\right) - \frac{15}{32}\deg(\Delta_E) - \frac{35}{24}. \qquad (7)$$

To bound $\deg(B'_n)$ above use the same tools. Note that the functoriality of the canonical height ensures $h = mh'$ with $m \geqslant 2$. Then

$$\deg(B'_n) < h'n^2 + \frac{3}{16}\deg(\Delta_{E'}) + \frac{5}{6} < \frac{h}{m}n^2 + \frac{3}{96}\deg(\Delta_E) + \frac{5}{6}. \qquad (8)$$

The right hand side of (8) is guaranteed to be smaller than the right hand side of (7) if

$$h\left(\frac{n^2}{m} - 1\right) > \frac{1}{2}\deg(\Delta_E) + \frac{55}{24}. \qquad (9)$$

Applying Lang's conjecture (Proposition 3.5, with c equal to the constant from there), n is guaranteed to be large enough if

$$n^2 \geqslant 4\left(1 + \frac{67}{24c}\right).$$

This shows that $\deg(B_n) > \deg(B'_n)$ for all $n \geqslant N_0$, say. Substituting in the values for c from Proposition 3.5 gives the stated values for N_0.

For the second inequality, again use Lemma 3.9 and Proposition 3.8. These give a lower bound for $\deg(B'_n)$ of the form

$$\frac{3}{4}h'n^2 - \frac{9}{32}\deg(\Delta_E) - \frac{15}{24}.$$

Similarly they give rise to an upper bound for $\deg(B_1)$ of the form

$$\deg(B_1) < h + \frac{3}{16}\deg(\Delta_E) + \frac{5}{6}.$$

Using the relation $h = mh'$, what we require is guaranteed if

$$h\left(\frac{3n^2}{4m} - 1\right) > \frac{15}{32}\deg(\Delta_E) + \frac{35}{24}. \qquad (10)$$

Using Lang's conjecture means we can guarantee $\deg(B'_n) > \deg(B_1)$ if

$$n^2 > m\left(1 + \frac{185}{96c}\right).$$

Inserting the various possibilities for c gives N_1. $\square$

3.6. **Explicit computations.** Given any particular example, it is possible to compute $h, \deg(\Delta_E)$ and m. This data can be fed into the bounds (9) and (10). Example 3.1 does not satisfy any of the special criteria in Theorem 3.12 so is best handled this way. The point $P = [t^2, t^2]$ on $E : y^2 = x^3 + t^2(1-t^2)x$ has global canonical height equal to $\frac{1}{2}$. It has bad reduction at t and is the image of a K-rational point under a 2-isogeny. This data is inserted into (9) and (10) to obtain a reasonable bound for the indices n beyond which B_n is reducible. Then the smaller indices can easily be checked.

On the other hand, the point $2P = [t^4 - t^2 + \frac{1}{4}, -t^6 + \frac{3}{2}t^4 - \frac{1}{4}t^2 - \frac{1}{8}]$ has good reduction away from infinity so Theorem 3.12 can be applied directly to obtain a reasonable bound. Then the smaller indices can be checked manually to verify that for all $n \geqslant 2$, the terms $B_n/B_1 = B_n$ have at least two distinct irreducible factors.

4. The rational case

Explicit results, when the base field is $\mathbb{Q}$, are harder to obtain. This is partly because Lang's conjecture is not known in general. The tables in Section 4.2 (see also Silverman [26, Exercise 6.10(d)]) give examples of rational points with very small ratio $\widehat{h}(P)/\log\Delta$, forcing the constant in Lang's conjecture to be small. This small constant plays a big role in the determination of an upper bound on the largest index yielding a prime and it makes a reasonable global uniform bound on the number of prime terms seem a very distant prospect. On the other hand it is possible to use our techniques to get reasonable bounds in particular cases, for example, for congruent number curves:

Example 4.1. [[9]] For

$$E : y^2 = x^3 - N^2x$$

with $5 \leqslant N \in \mathbb{N}$ square-free, assume P lies in the image of a 2-isogeny and has $x(P) < 0$, then each term B_n/B_1 fails to be a prime power for all $n \geqslant 8$. If P is integral then B_n fails to be a prime power for all $n \geqslant 3$. The conditions stated seem to be fulfilled for quite a few examples with small N. For example when $N = 5$ and $P = [-4, 6]$ (because $-4 + 5$ is a square). Similarly when $N = 6$ and $P = [-2, 8]$. Frustratingly, each curve also gives rise to elliptic divisibility sequences which are untouchable by our methods; even to the extent that we cannot prove that only finitely many terms are prime.

The heuristic argument in [5] predicts a bound for the number of prime terms in an elliptic divisibility sequence, provided the underlying curve is in minimal form. That argument can be sharpened by making an assumption coming from Diophantine analysis to predict a uniform bound; the details are given in section 4.1 below. However it cannot be adjusted to predict a uniform bound upon the index which yields the largest prime term. Although no such a bound is expected in general, a uniform bound in the

magnified case is not out of the question. The crucial issue lies within the realm of Diophantine approximation and will be discussed now.

4.1. **Heuristic argument.** The Prime Number Theorem suggests that the probability a large integer N is prime is roughly $1/\log N$. Therefore, if $(x_n)_{n\geqslant 1}$ is an increasing sequence of positive integers, this suggests that (in the absence of an obvious reason to believe otherwise), the expected number of prime terms x_n, with $n \leqslant X$, is approximately

$$\sum_{n\leqslant X} \frac{1}{\log x_n}. \tag{11}$$

In particular, one should suspect that x_n is prime infinitely often if and only if the sum in (11) diverges as $X \to \infty$. If $x_n = (a^n - b^n)/(a-b)$, then

$$\log x_n \sim nh(a/b) \text{ as } n \to \infty,$$

and so the sum diverges like a constant multiple of $\log X$. All the available evidence supports the belief that a sequence of this form with a and b not both k^{th} powers of integers, for some $k > 1$, will produce prime terms at that rate. If $x_n = B_n/B_1$, on the other hand,

$$\log x_n \sim n^2 \hat{h}(P) \text{ as } n \to \infty,$$

where $\hat{h}(P)$ is the global canonical height of P. As a consequence, the sum in (11) converges, and it seems likely that B_n/B_1 is prime only finitely often.

A sharpened version of this heuristic argument can be given. Using David's Theorem [4] from elliptic transcendence theory, it was argued in [6] that a lower bound for $\log B_n$ of the following kind holds:

$$\log B_n > hn^2 - C \log n (\log\log n)^4. \tag{12}$$

The dependence of the constant C is interesting. Suppose E is minimal and $C = O(h(E))$. Then Lang's conjecture implies that the sum in (11) is uniformly bounded above: in other words, for elliptic divisibility sequences coming from curves in minimal form, the sequence with n^{th} term B_n/B_1 should be a prime a uniformly bounded number of times. Note that this argument does not suggest a uniform bound upon the largest index n which yields a prime term B_n/B_1. Although David's Theorem is very strong, currently the best form of the constant C has a polynomial but non-linear dependence upon $h(E)$. If a version of (12) could be proved with a linear dependence on $h(E)$ then, together with Lang's conjecture, we obtain a heuristic justification for the uniform primality conjecture in general.

Failing this, a form of (12) with a smaller main term but a linear dependence in the error term would be adequate. This technique has been used a number of times. This was precisely the issue in the case when $K = \mathbb{Q}(t)$. In this case, a lower bound for $\deg(B_P)$ in terms of the height was given in Lemma 3.9. This is weaker than the equivalent form of (12) in that the leading term is only $\frac{3}{4}$ of what it might be. On the other hand, the error term is linear in $h(E)$ (or $\deg(\Delta_E)$). A similar device was exploited in [8]

to obtain a uniform primitive divisor theorem. In [8], the main term in (12) was replaced by a term only $\frac{1}{4}$ of what it might be. Any attempt to prove Conjecture 1.2 is likely to encounter this phenomenon.

4.2. **Explicit computations.** Here are presented prime terms in sequences generated by the rational points with smallest known height, in 18 cases drawn from Elkies' tables. The computations were performed using Pari-GP [21] (for the first 6 cases) and MAGMA [17] (for the other 12). In the table,

- E is an elliptic curve given by a minimal equation as a vector $[a_1, \dots, a_6]$ in Tate's notation;
- P denotes a non-torsion point in $E(\mathbb{Q})$;
- $(B_n)_{n\in\mathbb{N}}$ denotes the elliptic divisibility sequence associated to P;
- h_0 denotes 1000 times the global canonical height of P
- c_0 denotes 10000 times the ratio $\widehat{h}(P)/h(E)$
- N_2 denotes the maximal index for which the primality of B_n has been tested;
- N_0 denotes the number of indices $n \leqslant N_2$ such that $B_n = 1$;
- N_1 denotes the number of indices $n \leqslant N_2$ such that B_n is a prime number;
- N_3 is the greatest index $n \leqslant N_2$ such that B_n is a prime number.

The largest prime obtained comes from the first pair: the point

$$P = [7107, 594946]$$

on the curve

$$E : y^2 + xy + y = x^3 + x^2 - 125615x + 61201397$$

yields a prime term B_{3719} with 26774 decimal digits.

Minimal model	Point P	h_0	c_0	N_0	N_1	N_2	N_3
$[1,1,1,-125615,61201397]$	$[7107,594946]$	4.45	1.06	15	32	4500	3719
$[1,0,0,-141875,18393057]$	[-386, -3767]	4.51	1.18	15	32	4900	1811
$[1,-1,1,-3057,133281]$	[591, -14596]	4.86	1.65	13	29	4700	541
$[1,1,1,-2990,71147]$	[27, -119]	4.98	1.84	14	32	4500	829
$[0,0,0,-412,3316]$	[-18, -70]	5.63	2.90	11	28	4300	317
$[1,0,0,-4923717,4228856001]$	[1656, -25671]	5.71	1.24	14	29	4300	419
$[1,0,0,-13465,839225]$	[80, 485]	5.77	17.2	15	25	3000	571
$[1,0,0,-21736,875072]$	$[-154,-682]$	5.92	17.1	12	25	3000	953
$[1,-1,1-1517,26709]$	$[167,-2184]$	6.03	25.7	13	22	3000	1283
$[1,0,0,-8755,350177]$	$[14,473]$	6.12	18.9	15	32	3000	401
$[1,-1,1,-180,1047]$	$[-1,35]$	6.42	37.1	12	27	3000	383
$[1,0,0,-59852395,185731807025]$	$[12680,1204265]$	6.56	12.0	13	21	3000	359
$[1,0,0,-10280,409152]$	$[304,-5192]$	6.62	20.2	13	32	3000	311
$[0,1,1,-310,3364]$	$[-19,52]$	6.70	36.7	12	20	3000	103
$[1,0,0,-42145813,105399339617]$	$[31442,5449079]$	6.78	14.8	14	21	3000	349
$[1,0,0,-25757,320049]$	$[-116,-1265]$	6.82	19.4	14	22	3000	83
$[1,0,0,-350636,80632464]$	$[352,748]$	6.91	16.6	13	22	3000	137
$[1,0,0,-23611588,39078347792]$	$[-3718,-272866]$	7.41	16.6	13	23	3000	109

References

[1] J. W. S. Cassels, *Lectures on Elliptic Curves,* London Mathematical Society Student Texts 24, Cambridge University Press, Cambridge, 1991.

[2] D. V. Chudnovsky and G. V. Chudnovsky, *Sequences of numbers generated by addition in formal groups and new primality and factorization tests,* Adv. in Appl. Math. 7 (1986), 385–434.

[3] G. Cornelissen and K. Zahidi, *Elliptic divisibility sequences and undecidable problems about rational points,* J. reine angewandte Math., too appear.

[4] S. David. *Minorations de formes linéaires de logarithmes elliptiques.* Mém. Soc. Math. France (N.S.), (62):iv+143, 1995.

[5] M. Einsiedler, G. Everest and T. Ward, *Primes in elliptic divisibility sequences,* LMS J. Comp. Math. 4 (2001), 1–13.

[6] G. Everest and H. King, *Prime powers in elliptic divisibility sequences*, Math. Comp. 74 (2005), 2061–2071.

[7] G. Everest, V. Miller and N. Stephens, *Primes generated by elliptic curves,*. Proc. Amer. Math. Soc. 132 (2004), 955–963.

[8] G. Everest, G. McLaren, and T. Ward, *Primitive divisors of elliptic divisibility sequences*, Journal of Number Theory **118** no. 1 (2006), 71–89.

[9] G. Everest, V. Mahé and J.Reynolds, *The uniform primality conjecture for congruent number curves*, preprint.

[10] N. Elkies, *Rational points with small height* `www.math.harvard.edu/~elkies/low_height.html`

[11] M. Hindry and J. Silverman, *The canonical height and integral points on elliptic curves,* Invent. Math. 93, No.2, (1998), 419–450.

[12] Marc Hindry and Joseph H. Silverman, *Diophantine Geometry.* Springer Graduate Texts in Mathematics, Volume 201, New York, 2000

[13] P. Ingram, *Elliptic divisibility sequences over certain curves*, J. Number Theory **123** (2007), 473–486.
[14] P. Ingram, *Multiples of integral points on elliptic curves*, preprint.
[15] P. Ingram, *A quantitative primitive divisor result for elliptic divisibility sequences*, preprint.
[16] P. Ingram and J. H. Silverman, *Uniform estimates for primitive divisors in elliptic divisibility sequences*, preprint.
[17] MAGMA, version V2.13, University of Sydney, `http://magma.maths.usyd.edu.au/magma/index.html`
[18] S. Lang, *Elliptic Curves Diophantine Analysis* Springer-Verlag, Grundlehren der mathematischen Wissenschaften,volume 231, Berlin-Heidelberg, 1978.
[19] D. W. Masser and G. Wüsholtz, *Estimating isogenies on elliptic curves.* Inventiones mathematicae **100** (1990), 1–24.
[20] B. Mazur, *Modular curves and the Eisenstein ideal,* IHES Publ. Math. **47** (1977), 33–186.
[21] PARI-GP, `http://www.parigp-home.de`
[22] J. Pesenti and L. Szpiro, *Inégalité du discriminant pour les pinceaux elliptiques à réductions quelconques.* Compositio Math. 120 (2000), 83-117.
[23] B. Poonen, *Hilbert's Tenth Problem and Mazur's Conjecture for large subrings of* $\mathbb{Q}$*,* J. Amer. Math. Soc. **16** no.4 (2003), 981–990.
[24] Rachel Shipsey. *Elliptic divisibility sequences.* PhD thesis, Univ. of London, 2000.
[25] J. H. Silverman, *The Arithmetic of Elliptic Curves,* Graduate Texts in Mathematics 106, Springer-Verlag, New York, 1986.
[26] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves,* Graduate Texts in Mathematics 151, Springer-Verlag, New York, 1994.
[27] J. H. Silverman, *A quantitative version of Siegel's Theorem: Integral points on elliptic curves and Catalan curves,* J. Reine Angew. Math. 378 (1987), 60–100.
[28] J. H. Silverman, *Wieferich's criterion and the abc-conjecture*, J. Number Theory **30** (1988), no. 2, 226–237.
[29] J. H. Silverman, *Common divisors of elliptic divisibility sequences over function fields,* Manuscripta Mathematica, 114 (2004), no. 4, 431–446.
[30] J. H. Silverman and N. Stephens *The sign of an elliptic divisibility sequence,* J. Ramanujan Math. Soc. 21 (2006), no. 1, 1–17.
[31] J. H. Silverman, *p-adic properties of division polynomials and elliptic divisibility sequences,* Math. Ann. 332 (2005), no. 2, 443–471.
[32] M. Streng, *Divisibility sequences for elliptic curves with complex multiplication*, preprint.
[33] Morgan Ward. *Memoir on elliptic divisibility sequences.* Amer. J. Math., 70 (1948), 31–74.
[34] K. Zsigmondy, Zur Theorie der Potenzreste. *Monatsh. Math.*, 3 (1892), 265–284.

(GE,VM+SS) School of Mathematics, University of East Anglia, Norwich NR4 7TJ, UK

(PI) Department of Mathematics, University of Toronto, Canada M5S 2E4
E-mail address: `g.everest@uea.ac.uk`
E-mail address: `pingram@math.utoronto.ca`
E-mail address: `v.mahe@uea.ac.uk`
E-mail address: `shaun.stevens@uea.ac.uk`